IN THE CLAIMS

Claims 1-21 are presented below, with claims 1-5, 8-15, and 18-21 pending. As shown below, claims 1, 4-5, 8-11, 14-15, and 18-19 have been amended, claims 6-7 and 16-17 have been canceled, and new claims 20-21 have been added.

1. (Currently Amended) Method for the authentication of data communicated from a originator to a destination,

wherein a keyed hashing technique is used, according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic hash function and the data are transmitted together with the digest of the hash function from the originator to the destination,

characterized in that

the data comprises temporal validity information representing the temporal validity of the data;

the originator receives an acknowledgement key from the destination, wherein the acknowledgement key includes a time stamp; and

the originator verifies the acknowledgment key on the basis of the time stamp and the temporal validity information.

2. (Original) Method according to claim 1,

characterized in that

the temporal validity information can be defined by the originator.

3. (Previously Presented) Method according to claim 1,

characterized in that

the data comprises random data which are unique for a time span defined by the temporal validity information.

4. (Currently Amended) Method according to claim 1,

characterized in that

the data is a login key for a communication setup ~~and/or a message~~.

5. (Currently Amended) Method for the authenticated transmission of messages,

comprising the following communication setup steps:

- generating a login key by a keyed-hashing method on the basis of random data, temporal validity information and a private key,

- transmitting the login key from an originator to a destination, and

- verifying the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest on the destination side; and

comprising the following acknowledgement steps:

in case the verification of the authenticity and the temporal validity of the login key is positive,

- generating an acknowledgment key by a keyed-hashing method on the basis of second random data and the private key, wherein the acknowledgement key includes a time stamp,

- transmitting the acknowledgment key from the destination to the originator, and

- verifying the acknowledgment key by the originator, including checking the acknowledgement key on the basis of the time stamp and the temporal validity information whether the acknowledgment key is still valid.

6. – 7. (Canceled)

8. (Currently Amended) Method according to claim ~~6~~5,

furthermore comprising the following message transmission steps:

in case the verification of the acknowledgment key is positive,

- extracting the second random data from the acknowledgment key,

- generating a message by a keyed-hashing method on the basis of the second random data, message data and the private key,

- transmitting the message from the originator to the destination, and

- verifying the message by the destination.

9. (Currently Amended) Method according to claim 8,

characterized in that

the message furthermore comprises a time stamp and when verifying the message it is checked on the basis of the time stamp of the message and the temporal validity information whether the message is still valid.

10. (Currently Amended) A software ~~Software~~ program product,

characterized in that

~~it~~ the software program product implements, when loaded into a computing device of a distributed system, a method according to claim 5.

11. (Currently Amended) Distributed system for communicating authenticated data from a originator to a destination,

designed for a keyed hashing technique according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic hash function, and the data are transmitted together with the digest of the hash function from the originator to the destination,

characterized in that

the data comprises temporal validity information representing the temporal validity of the data;

the originator receives an acknowledgement key from the destination, wherein the acknowledgement key includes a time stamp; and

the originator verifies the acknowledgment key on the basis of the time stamp and the temporal validity information.

12. (Original) Distributed system according to claim 11,

characterized in that

the originator is designed to define the temporal validity information.

13. (Previously Presented) Distributed system according to claim 11, characterized in that the data comprises random data which are unique for a time span defined by the temporal validity information.

14. (Currently Amended) Distributed system according to claim 11, characterized in that the data is a login key for a communication setup ~~and/or a message~~.

15. (Currently Amended) Distributed system for the authenticated transmission of messages, comprising:

- an originator designed to generate a login key by a keyed-hashing method on the basis of random data, temporal validity information and a private key, wherein the login key includes a keyed hashing digest; and

- a network for transmitting the login key from the originator to a destination, wherein the destination is designed to verify the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest;

wherein the destination is designed to generate an acknowledgment key by a keyed-hashing method on the basis of second random data and the private key and to transmit the acknowledgment key to the originator in case the verification of the authenticity and the temporal validity of the login key is positive, and the acknowledgement key includes a time stamp.

the originator is designed to verify the acknowledgment key, including checking on the basis of the time stamp and the temporal validity information whether the acknowledgment key is still valid.

16. – 17. (Canceled)

18. (Currently Amended) Distributed system according to claim ~~16~~15,
characterized in that
the originator is designed to extract the second random data from the acknowledgment key in case the verification of the acknowledgment key is positive, generate a message by a keyed-hashing method on the basis of the second random data, message data and the private key, and transmit the message to the destination, and the destination is designed to verify the message.

19. (Currently Amended) Distributed system according to claim 18,
characterized in that
the message furthermore comprises a time stamp and when verifying the message, the destination checks on the basis of the time stamp of the message and the temporal validity information whether the message is still valid.

20. (New) Method according to claim 1,
characterized in that
the data is a message.

21. (New) Distributed system according to claim 11,

characterized in that

the data is a message.